DPA Leakage Models for CMOS Logic Circuits

Daisuke Suzuki[1], Minoru Saeki[1], and Tetsuya Ichikawa[2]

[1] Mitsubishi Electric Corporation, Information Technology R&D Center,
{dice, rebecca}@iss.isl.melco.co.jp
[2] Mitsubishi Electric Engineering Company Limited, Kamakura Office,
ichikawa@kam.mee.co.jp

Abstract. In this paper, we propose new models for directly evaluating DPA leakage from logic information in CMOS circuits. These models are based on the transition probability for each gate, and are naturally applicable to various actual devices for simulating power analysis. We also report the effectiveness of the previously known enhanced DPA on our model. Furthermore, we demonstrate the weakness of previously known hardware countermeasures for both our model and FPGA and suggest secure conditions for the hardware countermeasure.

1 Introduction

SPA (Simple Power Analysis) and DPA (Differential Power Analysis), proposed by P.Kocher, have become a threat to the security of cryptographic implementation such as SmartCard [1]. Ever since these proposals, cryptographic researchers have begun to consider not only mathematical attacks but side-channel attacks as well. This work has resulted in several proposed countermeasures, particularly against DPA. These countermeasures can be roughly classified into the following two groups:

- Algorithmic level
- Circuit level

Coron addresses countermeasures for public-key encryption algorithms [2]. Employing masked data with random numbers, Akkar uses countermeasures for block ciphers [3]. We consider the above mentioned examples to be algorithmic. On the other hand, SABL (Sense Amplifier Based Logic) [4][5] based on the DCVSL (Differential Cascode Voltage Switch Logic), SDDL (Simple Dynamic Differential Logic) based on the CMOS circuit using the SABL methodology, and WDDL (Wave Dynamic Differential Logic) [6] belong to the circuit level.

Generally, ASICs, such as microprocessors and cryptographic co-processors, are implemented based on the CMOS technology. We believe that countermeasures at the circuit level, such as WDDL and Masked-AND [7], are the most fundamental techniques because these are related to power consumption and are applicable to various cryptographic algorithms.

The manner in which the effectiveness of a countermeasure can be demonstrated is important. In this paper, we consider a methodology for the security

evaluation of CMOS circuits at the outset. Some attempts have already been made to systematically analyze DPA leakage [8][9][10]. Constructing a power consumption model is an effective method for the analysis of the effectiveness of countermeasures. For instance, the model based on the analog characteristics of CMOS circuits [8], the model based on the Hamming weight [9], and the simplification model in Ref. [8] based on the transition of data registers [10] were proposed in 1999, 2000, and 2002, respectively. Each model is complex or insufficient in terms of the reason for the leakage, because the aim of the model is to simulate power consumption itself or to determine the bias of data, not the bias of power consumption. We now present new models that determines the origin of the leakage. These models are based on signal transition probability for each gate(see also [11]), and are not only more accurate than the digital model [9] but are also more easily applicable than the analog models [8][10]. We will point out that the evaluation results of some primitive logics using our models are very similar to the actual power analysis using FPGA.

Next, we discuss the relation between *enhanced DPAs* and our leakage model. Recently, various analysis technics were proposed as enhanced DPA [12][13]. The countermeasure should satisfy the requisite tolerance for these technics. In this paper, we also discuss the effectiveness of the previously known enhanced DPAs from the viewpoint of our model.

Finally, we demonstrate the weakness of previously known hardware countermeasures for both our model and FPGA and suggest secure conditions on the CMOS logic circuit.

2 Leakage Model for CMOS Circuit

The current evaluation model against DPA is constructed by simulating the power consumption of the circuit. In general, there are two approaches. One method constructs a detailed model of a characteristic of the analog device [8][10]. In this case, the power consumption can be estimated with high accuracy. However, the estimation of the power consumption is largely dependent on the device; thus, it tends to become complex. The other method roughly estimates the power consumption assuming a certain digital model; for example, it estimates the power consumption based on the Hamming weights [12]. In this approach, it is possible to construct simple models and evaluate power consumption without device dependency. However, the result might not accurately reflect the behavior of the actual device.

In the following section, we propose a more detailed model that improves on the flipping model introduced in Ref. [15] for CMOS circuits. Hereafter, we refer to this model as the *leakage model*. The primary concept of the model is mainly to evaluate only the leakage information for DPA. Power consumption itself is not considered in this model.

2.1 Leakage Model Based on Transition Probability

Power consumption in CMOS circuits is summarized by the following equation [16]:

$$P_{\text{total}} = p_{\text{t}} \cdot C_{\text{L}} \cdot V_{\text{dd}}^2 \cdot f_{\text{clk}} + p_{\text{t}} \cdot I_{\text{sc}} \cdot V_{\text{dd}} \cdot f_{\text{clk}} + I_{\text{leakage}} \cdot V_{\text{dd}}, \tag{1}$$

where C_{L} is the loading capacitance, f_{clk} is the clock frequency, V_{dd} is the supply voltage, p_{t} is the transition probability of the signal, I_{sc} is the direct-path short circuit current, and I_{leakage} is the leakage current.

The first term results from the charge/discharge of the loading capacitance. The second term depends on I_{sc}, which arises when both the NMOS and PMOS transistors are simultaneously active. The third term represents power consumption caused by the leakage current, which is primarily determined by the characteristics of the CMOS process.

DPA is an attack in which the attacker estimates the intermediate value in the encryption/decryption process, classifies the patterns of power consumption based on this estimate, and obtains the secret information from the measured differences. Here, only p_{t} is dependent on the intermediate value in Eq.(1). Other parameters are fixed when the circuit is constructed. We assume that the power difference in DPA measurements occurs because the transition probability of the signal is biased according to the intermediate value. A detailed discussion of the bias of the transition probability is presented below.

Generally, the signal transitions also depend on the delay in the transistors and the wiring in the CMOS device as well as on the logic functions of the circuits. Thus, we consider the leakage model in either of the following cases:

- *Static Model* : An ideal circuit with no delay and transient hazard in transistor and wiring.
- *Dynamic Model* : A real circuit wherein a transient hazard is generated due to the delay.

In order to clarify the discussion, we analyze the generalized circuit as shown in Fig. 1. This circuit is constructed with k gates and n inputs x_1,x_2,...,x_n and feedback paths from the combinational circuit to the registers. The transition of the output signal at the ith gate is expressed as

$$\Delta f_{(i)} = f_{(i)}(x_1 \oplus \Delta x_1, \cdots, x_n \oplus \Delta x_n) \oplus f_{(i)}(x_1, \cdots, x_n), \tag{2}$$

where Δx is a transition of the input signal and f_i is a Boolean function at the output of the ith gate. In the following section, we define the leakage model by considering the bias of the probability of $\Delta f_{(i)} = 1$ in cases where $\alpha = 0$ or $\alpha = 1$, with α being the value of the signal used by the attacker for grouping. We will refer to this signal a *selection bit*.

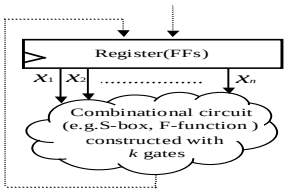

Fig. 1. General combinational circuit

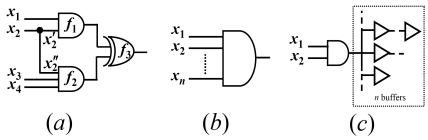

Fig. 2. Sample circuits (*a*) AND-XOR, (*b*) n-AND, and (*c*) 2-AND with n-buffer

2.2 Static Leakage Model

We assume that x_1,x_2,...,x_n in Fig. 1 are independent variables [3]. In the static model, the expectation of the transition frequency in one clock cycle is expressed as

$$N_{\alpha}^{\mathrm{stc}} = \sum_{i=1}^{k} p_{\alpha,(i)}^{\mathrm{stc}}, \tag{3}$$

where $p_{\alpha,(i)}^{\mathrm{stc}}$ is the transition probability at the output of the ith gate corresponding to the value of the selection bit α.

Definition 1. (Static Leakage) *Static leakage $N_{\mathrm{diff}}^{\mathrm{stc}}$ in the combinational circuit is*

$$N_{\mathrm{diff}}^{\mathrm{stc}} = N_{\alpha=1}^{\mathrm{stc}} - N_{\alpha=0}^{\mathrm{stc}} = \sum_{i=1}^{k} (p_{\alpha=1,(i)}^{\mathrm{stc}} - p_{\alpha=0,(i)}^{\mathrm{stc}}), \tag{4}$$

where $p_{x,(i)}^{\mathrm{stc}}$ is the transition probability of $\Delta f_{(i)} = 1$ under the condition that $\Delta x_1, ..., \Delta x_n$ are n independent variables.

If $N_{\mathrm{diff}}^{\mathrm{stc}} \neq 0$, it is possible that the correlation peak is observed in DPA measurements from Eq. (1). Generally, a normal nonlinear logic using a CMOS standard cell library has $N_{\mathrm{diff}}^{\mathrm{stc}} \neq 0$. Some examples are provided below.

Example 1: AND-XOR We consider the static leakage in Fig. 2 (*a*) with random inputs. If the selection bit is x_1, we get

$$\begin{aligned}
\Delta f_{(1)} &= x_1 \cdot \Delta x_2 \oplus x_2 \cdot \Delta x_1 \oplus \Delta x_1 \cdot \Delta x_2, \\
\Delta f_{(2)} &= x_2 \cdot x_3 \cdot \Delta x_4 \oplus x_3 \cdot x_4 \cdot \Delta x_2 \oplus x_4 \cdot x_2 \cdot \Delta x_3 \oplus x_2 \cdot \Delta x_3 \cdot \Delta x_4 \\
&\quad \oplus x_3 \cdot \Delta x_4 \cdot \Delta x_2 \oplus x_4 \cdot \Delta x_2 \cdot \Delta x_3 \oplus \Delta x_2 \cdot \Delta x_3 \cdot \Delta x_4, \\
\Delta f_{(3)} &= \Delta f_{(1)} \oplus \Delta f_{(2)}.
\end{aligned} \tag{5}$$

[3] These are not strictly independent, but any variation from independence is negligible when the bias of the transition probability for each gate is discussed in a cryptographic circuit.

Namely,

$$\Delta f_{x_1=1,(1)} = \Delta x_2 \oplus x_2 \cdot \Delta x_1 \oplus \Delta x_1 \cdot \Delta x_2,$$
$$\Delta f_{x_1=0,(1)} = x_2 \cdot \Delta x_1 \oplus \Delta x_1 \cdot \Delta x_2.$$

$x_i = 1$ and $\Delta x_i = 1$ occur with a probability 1/2. Here, the input states $(x_2, \Delta x_1, \Delta x_2)$ that assume $\Delta f_{x_1=1,(1)} = 1$ are (0,0,1), (1,0,1), (1,1,0), and (1,1,1). Hence, we have

$$p^{\mathrm{stc}}_{x_1=1,(1)} = 1/2,\ p^{\mathrm{stc}}_{x_1=0,(1)} = 1/4.$$

Similarly,

$$p^{\mathrm{stc}}_{x_1=1,(2)} = 7/32,\ p^{\mathrm{stc}}_{x_1=0,(2)} = 7/32,\ p^{\mathrm{stc}}_{x_1=1,(3)} = 7/16,\ p^{\mathrm{stc}}_{x_1=0,(3)} = 5/16.$$

Thus, the static leakage in Fig.2 (a) is

$$N^{\mathrm{stc}}_{\mathrm{diff}} = 3/8.$$

The fact that AND-XOR is a basic element for S-boxes implies that a normal implementation of a block cipher necessarily has static leakage.

Example 2: n-AND Under a condition similar to that in Example 1, the static leakage of n-input AND gates shown in Fig. 2 (b) is

$$N^{\mathrm{stc}}_{\mathrm{diff}} = (2^{n-1} - 1)/2^{2n-2},$$

where the selection bit $\alpha \in \{x_1, \cdots, x_n\}$.

Example 3: Buffer Tree The static leakage of two-input AND gates connected to n buffers (Fig. 2 (c)) is

$$N^{\mathrm{stc}}_{\mathrm{diff}} = \frac{1}{4} \cdot n,$$

where the selection bit is x_1 or x_2. Stated simply, the static leakage at the gate with a large fan-out is amplified.

Based on Definition 1, the static leakage has the property described in the following section.

Property 1: Consecutive Static Leakage *An equal amount of static leakage occurs both in the cycle when the selection bit appears and in the next cycle.*

Based on Eq. (2), it is evident that the transitions related to the selection bit occur in the cycle when the selection bit appears and in the next cycle as well. In cryptographic circuits, Δx_1,...,Δx_n are generally independent random variables. Thus, two static leakages of equal amounts occur for two consecutive cycles because two biased state transitions occur (random state $\rightarrow$ state dependent on α, state dependent on $\alpha \rightarrow$ random state). This implies that two similar DPA peaks are observed for two consecutive clock cycles in the DPA measurements if the target device is ideal.

2.3 Dynamic Leakage Model

In an actual cryptographic circuit, the delay time depends on the signal route. In addition, each route tends to be non-uniform. Such non-uniformity is particularly remarkable in the circuits designed with automatic synthesis/layout.

As in Section 2.2, we consider the transition probability in Fig. 1. We assume that the transitions $\Delta x_1, ..., \Delta x_n$ of the registers reach each gate at different times. Here, the transition of the Boolean function $\Delta f_{(i)}$ occurs only when transitions of the registers reach the ith gate. Based on these facts, we can evaluate the transition probability at a certain timing by supposing that only the transition corresponding to the timing is a variable and that others are 0. We define *Dynamic Leakage* using this probability.

Definition 2. (Dynamic Leakage) *Let Δt be a time interval that an attacker can observe. Dynamic leakage $N_{\mathrm{diff}}^{\mathrm{dyc}}$ in Δt on the combinational circuit is*

$$N_{\mathrm{diff}}^{\mathrm{dyc}} = N_{\alpha=1}^{\mathrm{dyc}} - N_{\alpha=0}^{\mathrm{dyc}} = \sum_{i=1}^{k} \sum_{e \in E(i)} (p_{\alpha=1,(i)}^{\mathrm{dyc}}(e) - p_{\alpha=0,(i)}^{\mathrm{dyc}}(e)), \tag{6}$$

where $E(i)$ is the set of events with the possibility that transition occurs in the state after α appeared at the ith gate in Δt, and $p_{\alpha,(i)}^{\mathrm{dyc}}(e)$ is the probability of $\Delta f_{(i)} = 1$ under the condition that the transition of the input signal corresponding to e is a variable and the others are 0.

Here, we consider the relation between the transitions of the registers Δx_1,..., Δx_n and the event $e \in E(i)$ that depends on the selection bit α. If the circuit has not been redundantly constructed and $\Delta t \geq 2$ cycles, $E(i)$ contains at least n events corresponding to the transitions of the registers in the state wherein α appeared. This does not depend on the order of the signal transitions. It should be noted that these events are distributed between two cycles according to the delay time, which was fixed when the circuit was constructed, for each signal to propagate. Additionally, it is possible for two or more transitions to occur by the same transition of the register if the propagation route is different. In this case, the transitions corresponding to each route are treated as independent variables in Eq. (2). In the following section, we evaluate the dynamic leakage in Fig. 2.

Example 4: AND-XOR We consider the circuit, shown in Fig. 2(a), on the dynamic model. If $\Delta t \geq 2$ cycles, we get

$$E(1) = \{e(\Delta x_1), e(\Delta x_2^{'})\}, \quad E(2) = \{e(\Delta x_2^{''}), e(\Delta x_3), e(\Delta x_4)\},$$

$$E(3) = \{e(\Delta x_1), e(\Delta x_2^{'}), e(\Delta x_2^{''}), e(\Delta x_3), e(\Delta x_4)\}.$$

Based on Eq.(6), Δf_3 at each event is

$$\Delta f_{(3)}(e(\Delta x_1)) = x_2 \cdot \Delta x_1, \ \ \Delta f_{(3)}(e(\Delta x_2^{'})) = x_1 \cdot \Delta x_2^{'}, \ \ \Delta f_{(3)}(e(\Delta x_2^{''})) = x_3 \cdot x_4 \cdot \Delta x_2^{''},$$

$$\Delta f_{(3)}(e(\Delta x_3)) = x_4 \cdot x_2 \cdot \Delta x_3, \quad \Delta f_{(3)}(e(\Delta x_4)) = x_2 \cdot x_4 \cdot \Delta x_3.$$

If x_1 is the selection bit, we have

$$p^{\mathrm{dyc}}_{x_1=1,(3)}(e(\Delta x_2^{'})) = 1/2, \quad p^{\mathrm{dyc}}_{x_1=0,(3)}(e(\Delta x_2^{'})) = 0.$$

Similarly, in $\Delta f_{(1)}$, we have

$$p^{\mathrm{dyc}}_{x_1=1,(1)}(e(\Delta x_2^{'})) = 1/2, \quad p^{\mathrm{dyc}}_{x_1=0,(1)}(e(\Delta x_2^{'})) = 0.$$

The dynamic leakage of Fig. 2(a) is $N^{\mathrm{dyc}}_{\mathrm{diff}} = 1$.

It should be noted that the difference between x_1 and $x_2^{'}$ at the delay time determines the timing whereby dynamic leakage occurs in the circuit. $N^{\mathrm{dyc}}_{\mathrm{diff}}$ occurs during the cycle when the predicted x_1 appears if $x_2^{'}$ is slower than x_1, and it occurs during the next cycle if the delay condition is converse.

Example 5: n-AND Under a condition similar to that in Example 4, the dynamic leakage, shown in Fig. 2 (b), is

$$N^{\mathrm{dyc}}_{\mathrm{diff}} = (n-1)/2^{n-1},$$

where $x \in \{\ x_1\ ,...,\ x_n\ \}$.

Finally, we describe a property common to static and dynamic leakage.

Property 2. (Complementary Leakage from AND- and OR-gate) *The static/dynamic leakages of an equal amount but of opposite polarity occur from thw AND- and OR-gate(or, the NAND- and NOR-gate) respectively, under the same input and delay time condition.*

This implies that there is the possibility that the leakage of the entire circuit is counterbalanced. In actuality, a countermeasure using this property has been proposed [17].

3 Enhanced Leakage Models

Thus far, some analysis technics that enhance standard DPA have been proposed. Here, we define the leakage model corresponding to these enhanced DPA and consider the effectiveness of each technic from the viewpoint of our model. In particular, we focus on Messerges's second-order DPA (M-2DPA) [12] and Waddle's second-order DPA (W-2DPA) [13] which are basically enhanced versions of DPA.

3.1 Standard Second-Order Attack

In standard DPA, the attacker analyzes power traces according to the average power difference at a specific time. On the other hand, in M-2DPA, the attacker analyzes power traces between two points. First, we define the leakage model of M-2DPA based on the signal transition in the following section.

Definition 3. (Leakage by Messerges's Second-Order DPA) *Let $N(t)$ be an expectation of the transition frequency at time t in the combinational circuit. Leakage by Messerges's second-order DPA $N_{\mathrm{diff}}^{\mathrm{2nd}}$ is*

$$N_{\mathrm{diff}}^{\mathrm{2nd}} = (N_{\alpha=1}(t') - N_{\alpha=1}(t)) - (N_{\alpha=0}(t') - N_{\alpha=0}(t)). \tag{7}$$

M-2DPA is an evaluation method that analyzes the correlation of the signal transition of two points. This implies that the correlation of the power consumption of two specific circuit components is evaluated. Moreover, this also implies that the correlation between cycles in the same circuit is evaluated if the combinational circuit is constructed with the loop architecture.

Next, we consider the condition to be secure against M-2DPA in CMOS logic circuits considering this leakage model. If a certain circuit is secure against standard DPA, the secure condition $N_{\mathrm{diff}} = 0$ is satisfied at any time in Eqs. (5) and (8). In this case, we have $N_{\alpha=1}(t) = N_{\alpha=0}(t)$ and $N_{\alpha=1}(t') = N_{\alpha=0}(t')$. Thus, this circuit obviously satisfies $N_{\mathrm{diff}}^{\mathrm{2nd}} = 0$. This implies that if the CMOS logic circuit is secure against standard DPA, it is also secure against M-2DPA. On the other hand, if a certain circuit is insecure against the standard DPA, we have $N_{\alpha=1}(t) - N_{\alpha=0}(t) = k_t (\neq 0)$ and $N_{\alpha=1}(t') - N_{\alpha=0}(t') = k_{t'}$ at any two points t and t', where k_t and $k_{t'}$ are the leakages against the standard DPA at each time. In this case, if $k_{t'} = k_t \neq 0$ is satisfied at any point, this circuit satisfies $N_{\mathrm{diff}}^{\mathrm{2nd}} = 0$. However, the circuit wherein equal leakage occurs at any point of time is not realistic. Namely, if the circuit is insecure against standard DPA, it is also insecure against M-2DPA in real circuits.

Taking the abovementioned facts into consideration using our models, we arrive at the following conclusion:

– Messerges's second-order DPA is an attack that is essentially equivalent to the standard DPA in CMOS logic circuits.

M-2DPA is useful only when the spike is made easily visible, the DPA trace with intuitive understanding is obtained, or the number of samples is decreased. In the construction of the hardware countermeasure, we have to consider only the the standard DPA.

3.2 Attack by Squaring Power Traces

Zero-Offset 2DPA, which was proposed by Waddle et al., is an analysis technic, which is characterized by the use of squaring power traces [13]. We will refer to this technic as the W-2DPA. In this section, we consider the effectiveness of W-2DPA from the viewpoint of our model.

Definition 4. (Leakage by Waddle's Second-Order DPA) *Let $S(t)$ be the set of transition frequencies with a possibility to occur at time t in the combinational circuit. Let $p_s(t)$ be the probability that the transition occurs in s gates at*

time t. The leakage by Waddle's Second-Order DPA V_{diff} is

$$V(t) = \sum_{s \in S(t)} (s^2 \cdot p_s(t)), \tag{8}$$

$$V_{\mathrm{diff}} = V_{\alpha=1}(t) - V_{\alpha=0}(t). \tag{9}$$

Here, we compare the secure condition of W-2DPA and standard DPA. Based on Definition 4, it is necessary to satisfy the following equation for $V_{\mathrm{diff}} = 0$.

$$\sum_{s \in S(t)} (s^2 \cdot p_{\alpha=1,s}(t)) = \sum_{s \in S(t)} (s^2 \cdot p_{\alpha=0,s}(t)) \tag{10}$$

In standard DPA, on the other hand, if $\sum(s \cdot p_{\alpha=1,s}(t))$ is equal to $\sum(s \cdot p_{\alpha=0,s}(t))$, $N_{\mathrm{diff}} = 0$ is satisfied. Thus, each secure condition is obviously different. This consideration suggests the following conclusion.

– Waddle's second-order DPA can detect the bias of the distribution of the transition probability in CMOS logic circuits.

W-2DPA is an analysis technic that is essentially different from standard DPA, and we must consider this technic in the construction of the hardware countermeasure. Actually, masked CMOS logics are weak against W-2DPA, even if the static model is assumed. These results are described in Section 4.

Next, we enhance Definition 4 more effectively. Generally, it is difficult to compute $p_s(t)$ in the entire circuit when the dynamic model is assumed. Therefore, we enhance Definition 4 such that it is applicable to the actual device for simulating power analysis.

Definition 5. (Enhanced Leakage by Waddle's Second-Order DPA) *Let Δt be a time interval that an attacker can observe. Let* TC *be the transition count to occur in Δt for the combinational circuit. Let* Nm *be the number of observed samples corresponding to α. Leakage by Waddle's Second-Order DPA V'_{diff} is*

$$V'_{\mathrm{diff}} = \left(\frac{\sum \mathrm{TC}^2}{\mathrm{Nm}}\right)_{\alpha=1} - \left(\frac{\sum \mathrm{TC}^2}{\mathrm{Nm}}\right)_{\alpha=0} \tag{11}$$

Our models which are based on the transition probability can evaluate the security strength of the circuit in advance by extracting the transition of each gate from the netlist [4] for the logic simulation. In Ref. [14], we point out that the evaluation results of logic simulation using our models are very similar to the actual circuits without countermeasures.

[4] A netlist is a text description of the circuit connectivity. It is basically a list of connectors, a list of instances (gates). In addition, the netlist can contain delay information.

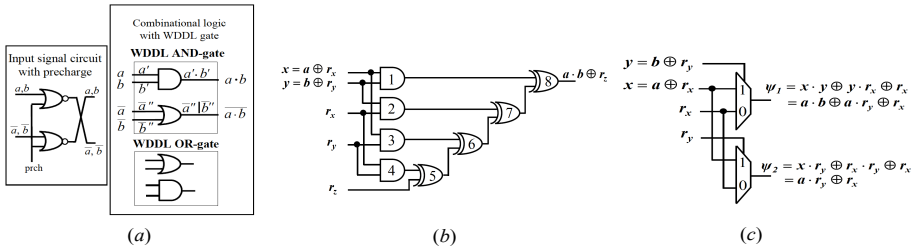

Fig. 3. Components of previously known countermeasures (a) WDDL, (b) Masked-AND, (c) MAND.

4 Evaluation for Previously Known Countermeasures

There are two approaches to the construction of countermeasures at the circuit level. The first approach uses complementary behavior and makes power consumption independent of data. The second uses data masking in combinational circuits and renders intermediate data unpredictable. In this section, we review a typical example based on each approach and evaluate each countermeasure by using our leakage models.

4.1 Previously Known Countermeasures on the CMOS Circuit

Wave Dynamic Differential Logic Tiri et al. proposed Wave Dynamic Differential Logic (WDDL) [6] which is based on dynamic and differential logic and constructed with CMOS standard cell libraries. Figure 3 (a) shows the basic components of WDDL. As the first step, WDDL executes a precharge at the beginning of the combinational logic. It only contains three logic gates, *i.e.*, AND, OR, and NOT. In addition, they proposed a method for the implementation of WDDL using FPGA.

Masked-AND Operation Figure 3 (b) shows the Masked-AND operation as proposed by Trichina [7]. Masked-AND is a method of calculating "$(a \cdot b) \oplus r_z$" using the above 5 input data, x, y, r_x, r_y and r_z. Hence, the computations, as shown in Fig. 3 (b), can be performed without compromising on the bits of actual data. In addition, Blömer et al. insist that this approach is "Provably Secure" against DPA in Ref. [19].

MAND Figure 3 (c) describes MAND proposed by Shimizu [18]. It is based on data masking and is characterized by the use of a dual-rail circuit.

4.2 Analysis for Complementary Logics

Based on Property 2, a complementary logic has the possibility of counterbalancing the leakage. WDDL is a method that refines this consideration. We consider

the circuit shown in Fig. 3 (a). At the end of the precharge phase (prch = 0), all output signals of the WDDL gates are at 0. Thus, the transitions for each gate in the evaluation phase (prch = 1) are equal to the wire value. In the case of the WDDL-AND gate,

$$\Delta f_{(AND)} = a \cdot b \quad \Delta f_{(OR)} = \bar{a} \mid \bar{b} = a \cdot b \oplus 1$$

Based on this, we obtain $N_{\mathrm{diff}}^{\mathrm{stc}} = 0$ because a transition occurs only at either one of the gates without any relation to the value of a or b.

Next, we consider the dynamic model. Here, we assume that the transition Δb arrives at the gates later than transition Δa. Table 1 shows the transition probability of each CMOS gate corresponding to each selection bit in this condition.

On the basis of the data listed in Table 1, if Δt in Definition 2 is long enough and both $e(\Delta a)$ and $e(\Delta b)$ occur for that time, $N_{\mathrm{diff}}^{\mathrm{dyc}} = 0$ is satisfied without any relation to the selection bit. However, if the attacker can observe power traces in Δt that contains $e(\Delta a)$, and not contain $e(\Delta b)$ [5], he can detect the bias of the transition frequency. It should be noted that it is difficult to observe the opposite case(only containing $e(\Delta b)$) because of some capacitance in the actual device. In the example of Table 1, the dynamic leakage of the WDDL-AND gate is $N_{\mathrm{diff}}^{\mathrm{dyc}} = -1$ in evaluation phase when a is the selection bit. Although it is necessary to consider all arrival sequences of input signals when conducting a more detailed evaluation, we omit the details here. In the precharge phase, the dynamic leakage of the WDDL-AND gate is $N_{\mathrm{diff}}^{\mathrm{dyc}} = 1$ for Table 1 when b is the selection bit and Δt contains $e(\Delta a)$, and not contain $e(\Delta b)$. It is noteworthy that the polarity of the leakage changes in the evaluation and precharge phases. In addition, the reason for the leakage of W-2DPA is similar to that mentioned above.

A similar observation applies to other countermeasures using complementary logic. On the basis of this consideration, the secure condition concerning complementary gates (logic) against DPA and W-2DPA is as follows:

– All input signals reach each complementary gate (logic) simultaneously.

Generally, it is difficult to implement this condition via circuits. In particular, it is not guaranteed in the LSI designed by the automatic synthesis/layout.

4.3 Analysis for Masked CMOS Logic

Generally, in order to extract the absolutely necessary results (e.g., $a \cdot b$) from the masked operation results (e.g., $(a \oplus r_x) \cdot (b \oplus r_y)$), the DPA countermeasures based on data masking need to operate some unnecessary terms (e.g., $(a \oplus r_x) \cdot r_y$). Several methods have been proposed regarding the manner in which the operations should be divided. In this section, we will consider and evaluate Masked-AND [7] and MAND [18].

[5] This implies that the attacker observes by using a higher sampling rate for the oscilloscope.

Masked-AND When evaluating the Masked-AND circuit with Definition 1, it satisfies $N_{\mathrm{diff}}^{\mathrm{stc}} = 0$ because the wire value of each gate is randomized as mentioned in Ref. [19]. On the other hand, when evaluating the circuit with Definition 2, there is a possibility that $N_{\mathrm{diff}}^{\mathrm{dyc}} \neq 0$. In Ref. [20], we analyze the abovementioned facts in more detail.

For this example, the output of gate 6 in Fig. 3 (*b*) is expressed as $x \cdot r_y \oplus r_x \cdot r_y \oplus z$. Here, if we assume that the signal transition occurs in order of x, r_x and r_y, the transition of gate 6 caused by $e(\Delta r_y)$ can be expressed as $x \cdot \Delta r_y \oplus r_x \cdot \Delta r_y = a \cdot \Delta r_y$. It follows that $p_{a=1,(6)}^{\mathrm{dyc}}(e(\Delta r_y)) = 1/2$, $p_{a=0,(6)}^{\mathrm{dyc}}(e(\Delta r_y)) = 0$. Thus, the leakage from gate 6 brought about by $e(\Delta r_y)$ is $N_{\mathrm{diff}}^{\mathrm{dyc}} = 1/2$. Furthermore, since an XOR-gate propagates transitions of its input signal, gate 7 whose input is the output of gate 6 causes the same leakage as that of gate 6. The same is also the case with gate 8.

As mentioned above, it can be stated that the Masked-AND circuit may have the bias of signal transition according to secret information when a certain delay condition is met. The leakage in the dynamic model of Masked-AND is also analyzed in Ref. [21], where a similar result is obtained.

Next, we discuss evaluating the Masked-AND circuit with Definition 5. For simplicity, we consider only four AND-gates in Fig. 3 (*b*) here. Table 2 lists the transition counts and their event probability when the selection bit is a, where $s \in \{0, 1, 2, 3, 4\}$ is the total transition count of these AND-gates.

The following can be qualitatively inferred from Table 1: If both a and b are 0, the four AND-gates from gate 1 to gate 4 in Fig. 3 (*b*), execute the same logical operation and often exhibit similar behavior. On the other hand, they often behave differently if a or b is not 0. Actually, the event probability of $s = 4$ is $p_4 = 7/64$ when $a = 0$, while it is $p_4 = 1/32$ when $a = 1$. In a similar manner, the event probability differs depending on a predictable signal value. Quantitatively, from Table 1 and Definition 5, $V'_{\mathrm{diff}} = -5/8$ when the selection bit is a or b. Therefore, the Masked-AND circuit can be attacked with W-2DPA.

MAND The same observation applies to MAND. Here, we describe the case that is not secure against W-DPA even if it is secure against standard DPA. We focus on the delay relation between the MUX data signals and the MUX select signals in MAND, and consider the leakage separately in the following two delay conditions:

- Condition 1 : "$\mathrm{delay}(y), \mathrm{delay}(r_y) < \mathrm{delay}(x), \mathrm{delay}(r_x)$"
  (or "$\mathrm{delay}(x), \mathrm{delay}(r_x) < \mathrm{delay}(y), \mathrm{delay}(r_y)$")

- Condition 2 : "$\mathrm{delay}(x) < \mathrm{delay}(y) < \mathrm{delay}(r_x)$" and
  "$\mathrm{delay}(x) < \mathrm{delay}(r_y) < \mathrm{delay}(r_x)$"
  (or "$\mathrm{delay}(r_x) < \mathrm{delay}(y) < \mathrm{delay}(x)$" and
  "$\mathrm{delay}(r_x) < \mathrm{delay}(r_y) < \mathrm{delay}(x)$")

Condition 1 states that transitions according to x and r_x occur at the events of the select signals. In addition, the condition in parentheses is a similar one, ex-

cluding the cycle when the transition occurs. Condition 2 states that transitions according to either x or r_x occur at the events of the select signals.

First, we evaluate the leakage in Condition 1. The transitions of ψ_1 and ψ_2 at the events of the select signals are

$$\Delta\psi_1(e(\Delta y)) = x \cdot \Delta y \oplus r_x \cdot \Delta y = a \cdot \Delta y,$$
$$\Delta\psi_2(e(\Delta r_y)) = x \cdot \Delta r_y \oplus r_x \cdot \Delta r_y = a \cdot \Delta r_y.$$

Namely, if the selection bit is a, we have

$$p^{\mathrm{dyc}}_{a=1,(\psi_1)}(e(\Delta y)) = 1/2,\ p^{\mathrm{dyc}}_{a=0,(\psi_1)}(e(\Delta y)) = 0,$$
$$p^{\mathrm{dyc}}_{a=1,(\psi_2)}(e(\Delta y)) = 1/2,\ p^{\mathrm{dyc}}_{a=0,(\psi_2)}(e(\Delta y)) = 0.$$

Thus, we evaluate the dynamic leakage of MAND as $N^{\mathrm{dyc}}_{\mathrm{diff}} = 1$. On the other hand, if the selection bit is b, it is evident that $N^{\mathrm{dyc}}_{\mathrm{diff}} = 0$.

Next, the transitions of ψ_1 and ψ_2 at the events of the select signals in Condition 2 are

$$\Delta\psi_1(e(\Delta y)) = x \cdot \Delta y \oplus r'_x,$$
$$\Delta\psi_2(e(\Delta r_y)) = x \cdot \Delta r_y \oplus r'_x,$$

where r'_x is the wire value of r_x at the previous state one cycle. In this case, it is evident that $N^{\mathrm{dyc}}_{\mathrm{diff}} = 0$ with any selection bit because random numbers are not canceled. Thus, MAND is secure against standard DPA under Condition 2.

Finally, we evaluate the leakage against W-2DPA. We show the probability distribution of MAND in the static model in Table 3. On the basis of this table, we have $V'_{\mathrm{diff}} = -1/4$. Thus, MAND is insecure against W-2DPA even if the static model is assumed.

Additionally, we consider the leakage against W-2DPA in Condition 2, which is secure against standard DPA. Although the data signal transitions influence both ψ_1 and ψ_2, the transitions of select signals influence only either one of the two. Since W-2DPA is an attack that paid attention to the distribution of the transition probability at the entire circuit, we consider the influence of the data signal transition here. The transitions of ψ_1 and ψ_2 at the events of the data signals in Condition 2 are $\Delta\psi_1(e(\Delta r_x)) = \Delta r_x \cdot y \oplus \Delta r_x, \Delta\psi_2(e(\Delta r_x)) = \Delta r_x \cdot r_y \oplus \Delta r_x$. Thus, the transition count is $s \in \{0, 2\}$ at $(e(\Delta r_x))$, assuming $b = 0$. Furthermore, each event probability is $p_0 = 3/4$ and $p_2 = 1/4$. On the other hand, the transition count is $s \in \{0, 1\}$ at $(e(\Delta r_x))$ assuming $b = 1$ and each event probability is $p_0 = 1/2$ and $p_2 = 1/2$. Therefore, since we have $V'_{\mathrm{diff}} = -1/2$, Condition 2 is insecure against W-2DPA even if it is secure against the standard DPA.

5 Experimental Results and Considerations

We evaluate the effectiveness of the previously known countermeasures by using FPGA. In this section, we show experimental results of elementary bricks of

Table 1. Transition probability of the WDDL-AND gate

α	CMOS gate	prch = 1		prch = 0	
		$e(\Delta a)$	$e(\Delta b)$	$e(\Delta a)$	$e(\Delta b)$
$a = 1$	AND	0	1/2	1/2	0
	OR	0	1/2	0	1/2
$a = 0$	AND	0	0	0	0
	OR	1	0	1/2	1/2
$b = 1$	AND	0	1/2	1/2	0
	OR	1/2	0	1/2	0
$b = 0$	AND	0	0	0	0
	OR	1/2	1/2	0	1

Table 2. Probability distribution of Masked-AND

Selection bit α	Transition count s	Event probability p_S
$a = 1$	0	5/32
	1	3/8
	2	5/16
	3	1/8
	4	1/32
$a = 0$	0	19/64
	1	3/16
	2	11/32
	3	1/16
	4	7/64

Table 3. Probability distribution of MAND

Selection bit α	Transition Count s	Event probability p_S
$a = 1$	0	1/4
	1	1/2
	2	1/4
$a = 0$	0	3/8
	1	1/4
	2	3/8

Table 4. Evaluation environment

Design environment	
Language	Verilog-HDL
Simulator	Verilog-XL
Logic synthesis	Synplify version 7.7
Place and Route	ISE version 6.3.03i
Measurement environment	
Target FPGA	XCV1000-6-BG560C
Oscilloscope	Tektronix TDS 7104

previously known countermeasures implemented on FPGA. The evaluation environment is the general one shown in Table 4. An XCV1000-6-BG560C FPGA of Xilinx Inc. is mounted on the target board. Additionally, automatic place-and-route tools were used for all layout design.

5.1 Standard DPA

Figure. 4 shows the experimental results of standard DPA for each countermeasure (i.e., normal-AND, WDDL, Masked-AND, and MAND).

In Fig. 4, the average power enlarges at time t_4 and time t_5 when the WDDL circuit is activated. The first half (t_4) is an evaluation phase, and the latter half (t_5) is a precharge phase of WDDL. Figure. 5 is a magnified view of the WDDL part in Fig. 4. There appears a small downward peak at time t_4 and a small upward peak at time t_5, each of which are caused by timing differences between the input signal a and input signal b because automatic place-and-route tools were used. These peaks are in good agreement with the forecast by the evaluation based on our leakage model.

The Masked-AND circuit is activated at time t_7 where an upward peak (as shown in the considerations in Section 4.3) is observed. Since this peak is caused by transient hazards, it is relatively small as compared to that of the normal-AND.

At time t_9, the MAND circuit is activated and an upward peak appears. As mentioned above, automatic place-and-route tools were used; thus, Condition 1 and Condition 2 shown in Section 4 are mixed. Therefore, leakage from Condition 1 can be observed. Here too, as in the Masked-AND case, the peak is relatively small as compared to that of the normal-AND because it is caused by transient hazards.

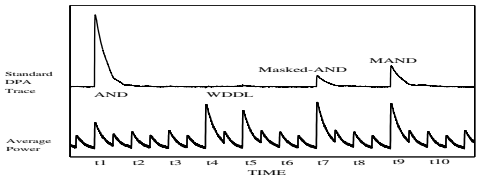

Fig. 4. Standard DPA result (200000 sample)

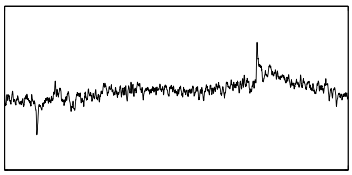

Fig. 5. Magnified view of the WDDL part in Fig.4

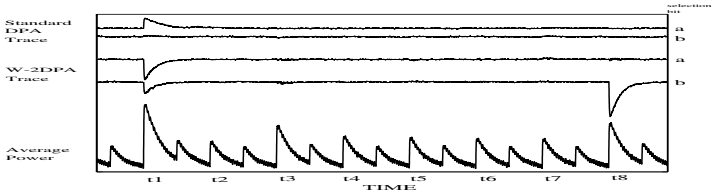

Fig. 6. Standard DPA and W-2DPA results for MAND (10000 sample)

In Fig. 6, the same MAND circuit as that in Fig. 4 is activated at time t_1. As evident from standard DPA traces in Fig. 6 at time t_1, leakage is observed when the selection bit is a, but it is not observed when the selection bit is b. The MAND circuit that satisfies Condition 2 is activated between time t_3 and time t_8 The MAND circuit that satisfies Condition 2 [6]. In this case, it is evident that leakage is not observed by standard DPA even if the selection bit is a. These results are in good agreement with the forecast in Section 4.

5.2 W-2DPA

Fig. 7 shows the experimental results of W-2DPA for each countermeasure (i.e., normal-AND, WDDL, Masked-AND, and MAND). The sample data used for the analysis is the same as the one used for standard DPA (Fig. 4). Fig. 8 is a magnified view of the WDDL part in Fig. 7. Peaks in Fig. 5 and Fig. 8 look similar, as indicated in the considerations in the previous section.

It should be noted that the peaks of Masked-AND and MAND are static in this case; hence, they are as large as that of normal-AND. In the case of starndard DPA, peaks of Masked-AND and MAND are caused by transient hazards; hence, they are not so large. In Fig. 6, W-2DPA traces between time t_3 and time t_8 show the experimental results of W-2DPA for the MAND circuit that satisfies Condition 2. While standard DPA traces show no peaks at time t_8, W-2DPA traces show a downward peak if the selection bit is b. This too is in good agreement with the considerations based on our leakage model.

[6] The condition is created by supplying input signals one by one for every clock cycle.

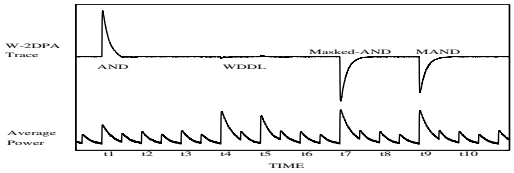

Fig. 7. W-2DPA result (200000 sample)

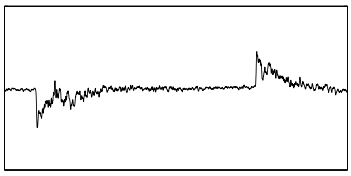

Fig. 8. Magnified view of the WDDL part in Fig.7

6 Toward a Perfect Countermeasure

Secure conditions of CMOS logic circuits against standard DPA and W-2DPA are $N_{\mathrm{diff}} = 0$ and $V'_{\mathrm{diff}} = 0$ without dependence on any selection bits.

The approach by complementary logics is very effective although the problem of the signal delay persists. Actually, the leakage of WDDL is the least in our experimental results. We predict that a manual layout strengthens WDDL.

The approach by data masking requires both main operation (e.g., $x \cdot y$) and cancel operation (e.g., $x \cdot r_y$, $y \cdot r_x$, and $r_x \cdot r_y$). When these operations are separately implemented by the CMOS logic gate, the probability distribution of the transition count in the entire circuit is different depending on sensitive information (see Section 5). A consideration of both the static model and dynamic model reveals that this fact occurs. Therefore, we suppose that it is difficult to resist various power analysis by the approach of data masking in a general CMOS gate. The solution to this is to construct a special CMOS gate, which is improved at the transistor level and satisfies secure condition. For further details of a countermeasure based on this consideration, see Ref. [11].

7 Conclusion

In this paper, we proposed leakage models of the CMOS logic circuits based on signal transition. These models are naturally applicable to various actual devices for simulating power analysis.

In addtiton, we evaluated the effectiveness of Messerges's second-order DPA (M-2DPA) and Waddle's second-order DPA (W-2DPA) from the viewpoint of our model. Thus, we demonstrated that M-2DPA is essentially equivalent to the standard DPA, and W-2DPA can detect the bias of the distribution of the transition probability in CMOS logic circuits.

Moreover, we analyzed previously known countermeasures by both our models and FPGA, and confirmed that the DPA traces on FPGA corresponded to the result obtained using our models. We emphasize the occurrence of the leakage in the previously known countermeasures. In particular, we pointed out that the masked CMOS logics have the similar weakness to standard CMOS logic without countermeasure against W-2DPA because the distribution of the transition probability are statically different.

References

1. P. Kocher, J. Jaffe and B. Jun, "Differential Power Analysis," *Crypto'99*, LNCS 1666, pp. 388-397, Springer-Verlag, 1999.
2. J.-S. Coron, "Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems," *CHES'99*, LNCS 1717, Springer-Verlag, pp. 292-302, 1999.
3. M. Akkar and C. Giraud, "An Implementation of DES and AES, Secure against Some Attacks," *CHES 2001*, LNCS 2162, pp. 309-318, Springer-Verlag, 2001.
4. K. Tiri, M. Akmal and I. Verbauwhede, "A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Power Analysis on SmartCards," Proc. of 28th European Solid-State Circuits Conference, pp.403-406, 2002.
5. K. Tiri and I. Verbauwhede, "Securing Encryption Algorithms against DPA at the Logic Level: Next Generation Smart Card Technology," *CHES 2003*, LNCS 2779, p.125-136, Springer-Verlag, 2003.
6. K. Tiri and I. Verbauwhede, "A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation," In Proc. of Design Automation and Test in Europe Conference, pp. 246-251, 2004.
7. E. Trichina, "Combinational Logic Design for AES SubByte Transformation on Masked Data," Cryptology ePrint Archive, 2003/236, 2003.
8. S. Chari, C.S. Jutla, J.R. Rao and P. Rohatgi, "Towards Sound Approaches to Counteract Power Analysis Attacks," *Crypto'99*, LNCS 1666, pp. 398-412, Springer-Verlag, 1999.
9. C. Clavier, J.-S. Coron and N. Dabbous, "Differential Power Analysis in the Presence of Hardware Countermeasures," *CHES 2000*, LNCS 1965, pp. 252-263, Springer-Verlag, 2000.
10. R. Bevan and E. Knudsen, "Ways to Enhance Differential Power Analysis," *ICISC 2002*, LNCS 2587, pp. 327-342, Springer-Verlag, 2003.
11. D. Suzuki, M.Saeki and T.Ichikawa, "Random Switching Logic: A Countermeasure against DPA based on Transition Probability," Cryptology ePrint Archive, Report 2004/346, 2004.
12. T.S. Messerges, "Using Second-Order Power Analysis to Attack DPA Resistant Software," *CHES 2000*, LNCS 1965, pp. 238-251, Springer-Verlag, 2000.
13. J. Waddle and D. Wagner, "Towards Efficient Second-Order Power Analysis," *CHES 2004*, LNCS 3156, pp. 1-15, Springer-Verlag, 2004.
14. M. Saeki, D. Suzuki and T. Ichikawa, "Construction of DPA Leakage Model and Evaluation by Logic Simulation," ISEC2004-57, IEICE, July 2004 (in Japanese).
15. M. Akkar, R. Bevan, P. Dischamp and D. Moyart, "Power Analysis, What Is Now Posible...," *Asiacrypto 2000*, LNCS 1976, pp. 489-502, Springer-Verlag, 2000.
16. A.P. Chandrakasan, S. Sheng and R.W. Brodersen, "Low Power Digital CMOS Design," IEEE Journal of Solid State Circuits, Vol.27, N0.4. pp. 473-484, 1992.
17. Philips Electronics NV, "DATA CARRIER WITH OBSCURED POWER CONSUMPTION," Patent, WO00/026746.
18. H. Shimizu, "A Countermeasure against Side Channel Attack using Mask Logic Elements," ISEC2004-69, IEICE, September 2004 (in Japanese).
19. J. Blömer, J.G. Merchan and V. Krummel, "Provably Secure Masking of AES," Cryptology ePrint Archive, Report 2004/101, 2004.
20. T. Ichikawa, D. Suzuki and M. Saeki, "An Attack on Cryptographic Hardware Design with Masking Method," ISEC2004-58, IEICE, July 2004 (in Japanese).
21. S. Mangard, T. Popp, and B. M. Gammel, " Side-Channel Leakage of Masked CMOS Gates", *CT-RSA 2005*, LNCS 3376, pp. 361-365, Springer-Verlag, 2005